AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND SEARCH WARRANT

I, Tim Loberg, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a state certified law enforcement officer employed as a Detective with the Waukesha County Sheriff's Department (WSD) and have been a sworn officer in the State of Wisconsin for approximately 13 years. I am currently assigned to the Waukesha County Drug Task Force. I am also a federally deputized Task Force Officer with the United States Department of Justice, Drug Enforcement Administration (DEA). As such, I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal felony offenses.

2. In connection with my official WSD and DEA duties, I investigate criminal violations of the Federal Controlled Substance laws, including, but not limited to Title 18, United States Code, Sections 924(c), 1956 and 1957; and Title 21, United States Code, Sections 841, 843, 846, 848, 952, and 963. I have been involved with various electronic surveillance methods, the debriefing of defendants, informants, and witnesses, as well as others who have knowledge of the distribution, transportation, storage and importation of controlled substances. I have participated in the execution of multiple search warrants.

3. I have received training in the area of controlled substances investigations, money laundering, financial investigations, and various methods that

drug dealers use in an effort to conceal and launder the proceeds of their illicit drug trafficking enterprises. I have participated in numerous investigations involving violations of state and federal controlled substances laws. I have participated or assisted in numerous federal and state search warrants for narcotic related offenses that have resulted in the seizure of United States currency, vehicles, real estate, and jewelry from individuals involved in narcotics trafficking.

4. I have authored and/or aided in investigations that have led to the issuance of numerous search warrants involving violations of both state and federal narcotic laws. These warrants involved the search of locations including residences of targets, their associates and relatives, "stash houses" (houses used as drug/money storage locations), storage facilities, bank safe deposit boxes, cellular/camera phones, and computers. Evidence searched for and recovered in these locations has included controlled substances, records pertaining to the expenditures and profits realized therefrom, monetary instruments, and various assets that were purchased with the proceeds of the drug trafficking.

5. Through training, experience, and discussions with other experienced agents:

a. I have learned about the manner in which individuals and organizations distribute controlled substances in Wisconsin as well as in other areas of the United States;

b. I am familiar with the appearance and street names of various drugs, including marijuana, heroin, methamphetamine, cocaine, and crack cocaine. I am familiar with the methods used by drug dealers to package and prepare controlled substances for sale. I know the street values of different quantities of the various controlled substances;

c. I am familiar with the coded language utilized over the telephone to discuss drug trafficking and know that the language is often limited, guarded, and coded. I also know the various code names used to describe controlled substances;

d. I know drug dealers often put telephones in the names of others (nominees) or obtain pre-paid cellular telephones from companies where no subscriber name or address is required to distance themselves from telephones that they use to facilitate drug distribution. Because drug traffickers go through many telephone numbers, they often do not pay final bills when they are done using a telephone number and then are unable to put another line in the name of that subscriber;

e. I know large-scale drug traffickers often purchase and/or title their assets in fictitious names, aliases, or the names of relatives, associates, or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in names other than the drug traffickers, the drug traffickers actually own and continue to use these assets and exercise dominion and control over them;

f. I know large-scale drug traffickers must maintain on-hand, large amounts of U.S. currency to maintain and finance their ongoing drug business;

g. I know it is common for drug traffickers to maintain books, records, receipts, notes, ledgers, airline tickets, and receipts relating to the purchase of financial instruments, and/or the transfer of funds and other papers relating to the transportation, ordering, sale, and distribution of controlled substances. That the aforementioned books, records, receipts, notes, ledgers, etc., are maintained where the traffickers have ready access to them;

h. I know it is common for large-scale drug traffickers to secrete contraband, proceeds of drug sales, and records of drug transactions in secure locations within their residences, their businesses, and/or other locations over which they maintain dominion and control, for ready access and to conceal these items from law enforcement authorities or rival drug traffickers. These secure locations include, but are not limited to safes, briefcases, purses, locked filing cabinets, and hidden storage areas in natural voids of a residence;

i. I know it is common for persons involved in large-scale drug trafficking to maintain evidence pertaining to their obtaining, secreting, transferring, concealing, and/or expenditure of drug proceeds, such as

currency, financial instruments, precious metals and gemstones, jewelry, books, records of real estate transactions, bank statements and records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashier's checks, bank checks, safe deposit box keys, and money wrappers. These items are maintained by the traffickers within residences (including attached and unattached garages), businesses or other locations over which they maintain dominion and control;

j. I know large-scale drug traffickers often use electronic equipment such as telephones (land-lines and cell phones), computers, telex machines, facsimile machines, currency counting machines, and telephone answering machines to generate, transfer, count, record and/or store the information described in the items above, as well as conduct drug trafficking activities;

k. I know when drug traffickers amass large proceeds from the sale of drugs, the drug traffickers attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize the following methods, including, but not limited to: domestic and international banks and their attendant services, securities brokers, professionals such as attorneys and accountants, casinos, real estate, shell corporations and business fronts, and otherwise legitimate businesses that generate large quantities of currency;

l. I know drug traffickers commonly maintain addresses or telephone numbers in books or papers that reflect names, addresses, and/or telephone numbers of their associates in the trafficking organization;

m. I know drug traffickers take or cause to be taken photographs of themselves, their associates, their property, and their drugs. These traffickers usually maintain these photographs in their possession; and

n. I know a "controlled buy" (and/or controlled contact) is a law enforcement operation in which an informant purchases drugs from a target. The operation is conducted using surveillance, usually audio and video taping equipment, and pre-recorded buy money. When an informant is used, he/she is searched for contraband, weapons, and money before the operation. The informant is also wired with a concealed body recorder and monitoring device. When the transaction is completed, the informant meets case agents at a pre-determined meet location and gives the purchased drugs and the recording/monitoring equipment to the case agents. The informant is again searched for contraband, weapons, and money. Additionally, all telephone calls made

by the informant while under the direction and control of case agents are recorded.

6. In addition, during the course of such residential searches, I and other agents have also found items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the subject premises. Such identification evidence is typical of the articles people commonly maintain in their residences, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys.

7. Pursuant to my official duties, I am submitting this affidavit in support of an application for a criminal complaint, arrest warrant, and search warrant for property described in Attachment A, for violations of federal law, including violations of Title 21, United States Code, Sections 841(a)(1), Distribution of, and Possession with Intent to Distribute, Controlled Substances; Title 18, United States Code, Section 924(c), Possession of Firearms in Furtherance of Drug Trafficking; and, Title 18, U.S.C. Section 2.

8. Throughout this affidavit, reference will be made to case agents. Case agents are those federal, state, and local law enforcement officers who have directly participated in this investigation, and with whom your affiant has had regular contact regarding this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

9. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing search warrants and a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations set forth above, occurred and that probable cause exists to believe that the property described in Attachment A, incorporated herein by reference, contain the items that are described in Attachment B.

II. INDIVIDUALS FOR WHOM A CRIMINAL COMPLAINT IS SOUGHT

	NAME	DATE OF BIRTH
1	Alfredo VARGAS RUIZ	[redacted]/1988

III. PROPERTIES FOR WHICH SEARCH WARRANTS ARE SOUGHT

10. For the reasons discussed herein, there is probable cause to believe that located at and in the following property, more fully described in Attachment A are items that constitute evidence of drug trafficking, including violations of Title 21, United States Code, Sections 841; and Title 18 United States Code, Sections 924(c), and 2.

a. [redacted], Milwaukee, WI – Primary residence of Alfredo VARGAS RUIZ. A check with WE Energies revealed

that there has been an open account at this address in the name of Ivonne Rivera, telephone number (414) 808-9083 since January 1, 2024.

10. I am submitting this affidavit in support of a Federal Criminal Complaint for Alfredo VARGAS RUIZ, H/M, DOB: [redacted]/1988, in the State and Eastern District of Wisconsin, as well as for a federal search warrant for VARGAS RUIZ's address, [redacted], Milwaukee, Wisconsin.

PROBABLE CAUSE

11. On Thursday September 19, 2024, at about 4:52 p.m., City of Greenfield Police Officers were dispatched to the area of South 33rd Street and West Loomis Road in reference to a hit on a stolen vehicle. Dispatch advised officers that a Kia Optima bearing Wisconsin registration ATR-7202 was being towed by a truck which was traveling westbound on West Loomis Road, and that this Kia Optima triggered a stolen vehicle alert.

12. Upon arrival to the area of the 3300 block of West Lomis Road, officers located the possible stolen Kia Optima. Officers observed that the Kia Optima was being towed on a trailer which was attached to a grey 2000 Dodge Ram 3500 pickup truck. Officers observed a male subject standing between the trailer and the truck as an officer drove past these vehicles while waiting for additional officers to respond. When other Greenfield Police Officers arrived to assist, the officers approached the Ram 3500 pickup truck. At this time, officers made contact with two subjects who were standing immediately outside of these vehicles. Officers identified these subjects as Jesus D. PEREA, DOB: [redacted], and Alfredo VARGAS RUIZ, M/H, DOB:

[redacted]/1988.

13. Officers asked PEREA if PEREA was with the vehicles in question (the Ram 3500 and the Kia Optima which was towed on the trailer). PEREA indicated that they were not PEREA's vehicles, and that PAREA was "helping another guy" who had just left. When officers asked PAREA how PAREA knows the referenced "guy," PAREA stated that PEREA did not know, and stated PAREA only knows VARGAS RUIZ. PEREA reported that this "guy" was a Hispanic male wearing a white shirt and black shorts who had driven the pickup truck to that location, but that this male had walked towards the nearby apartment buildings. Officers advised PAREA that the Kia was stolen, and asked PAREA who was driving the Ram 3500 pickup truck. PAREA eventually told officers that PAREA was the passenger in the Ram 3500, and that VARGAS RUIZ had been driving the vehicle.

14. Officers observed that the Ram 3500 pickup truck did not display any Wisconsin registration plates; however, the vehicle had Vehicle Identification Number (VIN) 1B7MC33W5YJ150623 affixed to it. A vehicle check of this VIN revealed to officers that the Ram 3500 pickup truck was entered as stolen through the City of Greenfield Police Department. While inspecting the Ram 3500 pickup truck further, officers observed shotgun shells in plain view stored in the driver's door handle compartment. With the stolen vehicle hit in place on the Ram 3500 pickup truck, both PEREA and VARGAS RUIZ were taken into custody.

15. Prior to being taken into custody, officers had also made contact with VARGAS RUIZ. VARGAS RUIZ told officers that VARGAS RUIZ had been walking

along West Loomis Road immediately prior to having contact with the officers regarding this incident. While walking, VARGAS RUIZ noticed that a white male whom VARGAS RUIZ did not know had been operating the Ram 3500 pickup truck. VARGAS RUIZ stated that this male needed help with attaching some straps onto the towed Kia Optima. VARGAS RUIZ stated that VARGAS RUIZ is a mechanic, and therefore offered to help this unidentified white male. VARGAS RUIZ also told officers that VARGAS RUIZ did not know PEREA, and when specifically asked by officers, VARGAS RUIZ denied operating or otherwise being in possession of the Ram 3500 pickup truck. When asked by officers where he walked from to get to the scene of the traffic stop, VARGAS RUIZ replied "home." When asked by officers where "home" was located, VARGAS RUIZ responded to officers that VARGAS RUIZ currently resided in the area of "16 and Windlake." Case agents believe this to be in reference to the intersection of S. 16th Street and W. Windlake Avenue, which is in close proximity to [redacted].

16. VARGAS RUIZ consented to a search of VARGAS RUIZ's person. While searching VARGAS RUIZ's person, officers located a key for a Dodge vehicle in VARGAS RUIZ's pocket. Officers confirmed that this particular key was for the ignition of the stolen Ram 3500 pickup truck, and when officers used the key, the Ram 3500 pickup truck started. When asked about this key, VARGAS RUIZ then told officers that VARGAS RUIZ was not the person who was driving the Ram 3500 pickup truck. VARGAS RUIS stated that VARGAS RUIZ noticed that the other individuals needed help with backing up the truck and trailer, therefore VARGAS RUIZ assisted

them only with backing up the ram 3500 pickup truck in order to park it. VARGAS RUIZ then told officers that VARGAS RUIZ turned the truck off once it was parked because exhaust fumes had been blowing into the faces of the people whom VARGAS RUIZ was assisting. In addition to the Ram 3500 pickup truck key, officers located a set of Kia keys in VARGAS RUIZ's pockets. Officers determined that these Kia keys unlocked the Kia Optima. Officers attempted to start the Kia Optima using the same Kia key, but it would not start because the battery was dead.

17. Officers learned that VARGAS RUIZ had an open felony case in Milwaukee County, with a bail restriction not to possess dangerous weapons or firearms or possess or use controlled substances without a prescription. While processing the scene of the stolen vehicles, officers observed drug paraphernalia near a sewer drain which was immediately next to the trailer in question, in an area where VARGAS RUIZ was standing when officers initially approached these vehicles. Officers recognized this paraphernalia to be associated with the usage of methamphetamine. After the arrests of VARGAS RUIZ and PEREA, officers searched the Ram 3500 pickup truck.

18. During the search of the Ram 3500, officers located a black bag on the passenger seat. In examining the contents of that bag, officers located another suspected methamphetamine pipe. Under the driver's seat, officers located an Ithaca 12-gauge shotgun, bearing serial number 8131604. Also under the driver seat was a green shopping bag containing other Ziploc bags of a white crystal-like substance, which officers suspected was methamphetamine, along with a glass pipe with a burnt

end which officers, based upon their training and experience, recognized as a "crack pipe." Officers also located and seized a Samsung cell phone which had been resting on the driver's side dashboard.

19. VARGAS RUIZ and PEREA were then conveyed to the City of Greenfield Police Department for further investigation and to be interviewed.

20. Once at the Greenfield Police Department, officers attempted a *Mirandized* interview with VARGAS RUIZ. VARGAS RUIZ declined to be interviewed.

21. Officers then conducted a recorded *Mirandized* interview of PEREA at the Greenfield Police Department. During that interview, PEREA advised that PEREA was picked up earlier in the day by VARGAS RUIZ at PEREA's residence located at [redacted] in the City of Milwaukee. VARGAS RUIZ drove to the Holt Park and Ride, where VARGAS RUIZ and PEREA picked up the stolen Kia Optima. PEREA stated that PEREA did not have knowledge that the Kia Optima was stolen and was told by VARGAS RUIZ that VARGAS RUIZ was picking up the car for a "client." When asked how long VARGAS RUIZ owned the Ram 3500 pickup truck, PEREA stated that PEREA believed VARGAS RUIZ had owned the truck for "a couple weeks." PEREA told officers that PEREA did not know either vehicle was stolen. PEREA stated that PEREA knows VARGAS RUIZ operates an automotive shop out of a storage unit which is located somewhere nearby 35th Street. Officers determined this storage unit to be the Storage Rentals of America Self-Storage facility located at 3645 West Loomis Road in the City of Greenfield. PEREA told

officers that PEREA knows VARGAS RUIZ sells drugs, and that, more specifically, PEREA has purchased crystal methamphetamine from VARGAS RUIZ in the past. PEREA recalled that approximately three to four days prior to this incident was the last time PEREA had purchased crystal methamphetamine from VARGAS RUIZ. PEREA also stated that earlier in the day when VARGAS RUIZ picked up PEREA, VARGAS RUIZ showed PEREA a "large amount of crystal meth." PEREA observed that VARGAS RUIZ stored the crystal methamphetamine in a green plastic bag. PEREA told officers that PEREA observed VARGAS RUIZ place the green plastic bag containing crystal methamphetamine into either the center console, or under the driver's seat of the Ram 3500 that VARGAS RUIZ and PEREA had been in. PEREA further stated that PEREA was aware that VARGAS RUIZ frequently supplied ounce quantities of methamphetamine to a subject unknown to PEREA, who resides at the [redacted] in the City of Milwaukee.

22. On September 24, 2024, at the request of Welks Automotive, City of Greenfield officers were dispatched to Welks Automotive, located at 7500 West Layton Avenue, Greenfield, Wisconsin, regarding the stolen Ram 3500. Upon being impounded there, Welks Automotive staff began searching the Ram 3500 truck, at which point they located the following:

- A fanny pack containing the following:
    - several keys for other vehicles;
    - 10.7 grams of suspected marijuana;
    - The Wisconsin Title for the Ram 3500 in question, with the

signature of the registered owner (Michael C. Dobson) forged onto it;

- An Illinois Registration Identification for an Atlas Trailer belonging to "Medved Asset Alliance LLC" of Wauconda, Illinois.

23. The Greenfield Police Department contacted the registered owner, Michael Dobson, and confirmed that Dobson had not signed the title despite his signature on the title. The Greenfield Police Department were therefore able to confirm that the signature was not from Dobson.

24. Officers later entered the evidence located in the Ram 3500 into evidence at the Greenfield Police Department. Among the items inventoried were approximately 156.48 gross grams of suspected methamphetamine, one Bullet Safe body armor, one pink key ring containing a Kia key, ten (10) 12-gauge shotgun shells and one (1) 9mm pistol round, two cellular telephones, and one Ithaca Model 37 12-gauge shotgun, bearing serial number 8131604.

25. Officers at the Greenfield Police Department subjected the suspected methamphetamine to a TruNarc Field test, and the results were positive for the presence of methamphetamine.

26. On October 1, 2024, officers at the Greenfield Police Department obtained and executed a search warrant on two cellular telephones seized during this investigation. These phones were described as a black Samsung cellphone in a black case (Greenfield Police Department property #24-002092-010) and a purple iPhone in a black case (Greenfield Police Department property #24-002092-011). Officers

recovered the purple iPhone in a black case (Greenfield Police Department property #24-002092-011) on VARGAS RUIZ's person at the time of VARGAS RUIZ's arrest. The forensic download of this phone showed the owner's name to be "Alfredo Vargas" with an Apple ID of "vargas.alfredo[redacted]" The telephone number of this device was [redacted]-8498.

27. An analysis of the data from the forensic download of VARGAS RUIZ's telephone number [redacted]-8498 revealed that many of the messages contained in the phone were in Spanish. Case agents, utilizing a Greenfield Police Officer who is fluent in Spanish, translated some of the messages from Spanish to English. Below are a few examples of messages contained in VARGAS RUIZ' cellular telephone.

28. On September 17, 2024, an individual referred to as "Joker111" contacted VARGAS RUIZ and stated, "Yo they need 2 ochos." Based upon my training and experience, as well as the translator verification, case agents know that the Spanish word for eight is "Ocho," and further believe that "ochos" is in reference to 1/8th ounce quantities of drugs, commonly referred to as an "eight ball." VARGAS RUIZ responded back "Estoy Aqui," which translates in English to "I am here or I'm here." VARGAS RUIZ then sent two more messages that stated "Yoo" and "Yooo." Approximately 46 minutes later, "Joker111" responded, "Yo my bad bro I had my phone on silent." Throughout the next half hour, various messages were sent back and forth. Among the messages "Joker111" sent "You still around," to which VARGAS RUIZ replied "Yes." "Joker111" sent a text "Bring me a ball," followed by "And let me see if my guy still needs them 2." VARGAS RUIZ responded, "Here" immediately

followed by "I come." "Joker111" replied, "Ok but can I give u 120 tomorrow morning bro because I forgot I had court today and I didn't make it to my guy to sell him my stamps before he went to work but he's coming at 10 am tomorrow to pick up the card and give me the 200 I'll give u 60 from the last stuff and 60 for this ball that's 120 for sure tomorrow morning is that koo?" Additionally, "My guy said tomorrow he wants the 2 that is too late for him to drive now." VARGAS RUIZ responded, "Ok." Based upon their training and experience, case agents believe that "Joker111" asked to purchase a 1/8-ounce quantity of drugs ("Bring me a ball") from VARGAS RUIZ, and that "Joker111" also asked to obtain two additional quantities of drugs for an associate ("And let me see if my guy still needs them 2") from VARGAS RUIZ. VARGAS RUIZ agreed to meet "Joker111" ("Here" and "I come") to provide the drugs.

29. On August 22, 2024, at approximately 5:29 a.m., an individual referred to as "Chakaloza" sent a text to VARGAS RUIZ. "If you got la shakaloza 100% I got u." VARGAS RUIZ immediately responded, "got u." "Chakaloza" replied immediately with a "heart emoji" to the message sent by VARGAS RUIZ, "got u." At approximately 7:59 p.m. that same day, "Chakaloza" responded to VARGAS RUIZ "akupan algodon." According to Spanish speaking officers, this text is translated into "do you need cotton." The officer stated that "Chakaloza" with a "ch" or "sh" in the beginning of the word is a Spanish term for a "party girl" and is also a Spanish term for cocaine. Further, "Algadon" (cotton) is also a Spanish term used to describe a white narcotic such as cocaine.

30. On August 23, 2024, at approximately 11:16 p.m., an individual referred

to as "Black 2" sent VARGAS RUIZ the following text. "Get me some Mary Jane and Yaya if u can." At approximately 11:21 p.m., "Black 2" also sent a text, "you got a dub on cashapp or perico I'm fucking hungry and shit." At approximately 12:49 a.m. on August 24, 2024, VARGAS RUIZ responded, "I'm going back to southside where are you." Based upon their training and experience, case agents believe that "Black 2" asked to purchase marijuana and cocaine ("get me some Mary Jane and Yaya if u can" and "you got a dub on cashapp or perico."). Case agents further know that "Yaya" is a slang term often used for cocaine. According to Spanish speaking officers, "perico" is a Spanish slang term for cocaine.

31. On July 18, 2024, at approximately 9:12 p.m., telephone number [redacted] 7797 (with no name associated to the number) sent VARGAS RUIZ "??." At approximately 10:19 p.m., the same telephone number sent VARGAS RUIZ a text, "Yo can you give me a ride to pik up some crico n I'll throw u some." On July 19, 2024, at approximately 5:38 a.m., VARGAS RUIZ sent "yooo," followed by "where are you guys" to the telephone number. At approximately 9:22 a.m., the same telephone number answered VARGAS RUIZ with "home." According to Spanish speaking officers, "crico" is a Spanish term used to describe crystal methamphetamine. Case agents therefore believe that the user of the telephone asked VARGAS RUIZ to give the user a ride to obtain methamphetamine. Following that, if VARGAS RUIZ gave the phone user a ride, the telephone user would provide VARGAS RUIZ with a portion of the methamphetamine ("yo can you give me a ride to pik up some crico n I'll throw u some.").

32. Case agents are aware that VARGAS RUIZ is charged in Milwaukee County Circuit Court under Case Number 2024CF001303, filed on March 18, 2024, with Drive or Operate Vehicle without Consent and Possession of Methamphetamine. According to Wisconsin Circuit Court records, VARGAS RUIZ has a listed address of [redacted] Milwaukee, WI 53215.

33. On September 30, 2024, Greenfield Police Department installed a remote video surveillance device that depicted the address of [redacted]. In reviewing the remote surveillance device, case agents have observed VARGAS RUIZ and/or vehicles associated with VARGAS RUIZ at the residence on a regular basis as recently as November 15, 2024. Additionally, based upon my training and experience, I know that drug traffickers commonly keep drug related items in their vehicles of ease of access.

V. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

54. Based upon my training and experience, I know that computer hardware and software may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime, and/or (2) the objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware and software which are (1) instrumentalities, fruits, or evidence of crime, or (2) storage devices for information about crime.

55. To this end, based upon my training and experience, I know that individuals involved in drug trafficking frequently use cellular telephones to maintain contact and arrange transactions with their sources and customers of and co-conspirators in the distribution of controlled substances. I have also found it very common for crime suspects to use their cellular telephones to communicate aurally or via electronic message in "text" format with individuals whom they purchase, trade, or otherwise negotiate to obtain illegal drugs. I also believe that it is common for crime suspects who possess illegal controlled substances and firearms to often take or cause to be taken photographs and other visual depictions of themselves, their associates, and the illegal controlled substances and firearms that they control, possess, buy, and sell.

56. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

57. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files

downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

58. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally,

some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to operate a website that is used for illegal conduct, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

59. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information.

Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

60. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

61. Because multiple people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be

found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

62. *Unlocking Apple brand devices:* I know based on my training and experience, as well as from information found in publicly available materials including those published by Apple, that Apple devices are used by many people in the United States, and that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

a. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

b. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and

(3) five unsuccessful attempts to unlock the device via Touch ID are made.

c. If Touch ID enabled Apple devices are found during a search of the PREMISES, the passcode or password that would unlock such the devices are presently unknown to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of any Apple device(s) found during the search of the PREMISES to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

d. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the premises to press their finger(s) against the Touch ID sensor of the locked Apple device(s) found during the search of the PREMISES in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID.

e. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the Apple device(s) found in the PREMISES as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

63. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the PREMISES to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad, found at the PREMISES for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

VI. CONCLUSION

64. Based on the forgoing, I believe there is probable cause to believe that Alfredo VARGAS RUIZ has and is committing violations of federal law, including Title 21, United States Code, Sections 841, and Title 18, United States Code, Sections 924(c), and 2. I further believe that there is probable to believe that located at and in the property described in Attachment A, there is evidence of drug trafficking, associated firearms possession, and fruits, instrumentalities and proceeds of drug trafficking, all of which is detailed more specifically in Attachment B, Items to be Seized.

ATTACHMENT B

Items To Be Seized

1. Paraphernalia associated with the manufacture and distribution of controlled substances including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances;

2. Duffel, canvas bags, suitcases, safes, or other containers to hold or transport controlled substances and drug trafficking related items and proceeds;

3. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;

4. Firearms, including pistols, handguns, shotguns, rifles, assault weapons, machine guns, magazines used to hold ammunition, silencers, components of firearms including laser sights and other components which can be used to modify firearms, ammunition and ammunition components, bulletproof vests, gun boxes and any and all documentation related to the purchase of such items;

5. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records and notes showing payment, receipt, concealment, transfer, or movement of money generated from the sale of controlled substances, or financial transactions related to the trafficking of controlled substances;

6. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;

7. Personal telephone books, address books, telephone bills, photographs, letters, cables, telegrams, facsimiles, personal notes, receipts, documents and other items or lists reflecting names, addresses, purchases, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in drug trafficking activities;

8. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;

9. Cellular telephones, text messaging systems, other communication devices, and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text messages, digital audio and/or video recordings, pictures, settings, and any other user defined settings and/or data, as well as any records associated with such communications services used to commit drug trafficking offenses;

10. Records, items and documents reflecting travel for the purpose of participating in drug trafficking activities, such as passports, airline tickets, bus tickets, vehicle rental receipts, credit card receipts, taxi cab receipts, hotel and restaurant receipts, canceled checks, maps, and records of long distance calls reflecting travel;

11. Indicia of occupancy, residency or ownership of the premises, vehicles, and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;

12. Photographs, videotapes or other depictions of assets, firearms, coconspirators, or controlled substances;

13. Computers, laptops, or other electronic storage device capable of being used to commit the violations or store any of the information described above.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).